CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

25 AUGUST 2017

(U) CALIFORNIA

(U) Los Angeles – Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack
(U) A Chinese national was arrested in Los Angeles this week on charges he used a rare type of computer malware that was also deployed to access millions of sensitive US records from the Office of Personnel Management (OPM). Court papers filed against Yu Pingan do not mention OPM, but they do suggest a connection between the two. The suspect, along with other conspirators in China, "would acquire and use malicious software tools, some of which were rare variants previously unidentified by the FBI and information security community, including a malicious software tool known as 'Sakula,' '' the criminal complaint states. The Sakula malware has previously been linked to the OPM hack, as well as other suspected computer system penetrations in the United States.
SOURCE: 24 August 2017, The Washington Post

(U) San Diego – Authorities Take 12 Migrants into Custody After Panga Boat Found
(U) A dozen people were apprehended trying to illegally enter the country off the coast of Mission Bay and Point Loma yesterday. US Customs and Border Protection (CBP) said the Joint Harbor Operation Center (JHOC) alerted agents to an area just west of Belmont Park where they observed a "panga-style" boat landing on the beach. About 10 people ran ashore, according to CBP, before the boat headed south. Border Patrol agents responded and were able to catch the 10 individuals. Minutes later, another panga-style boat was spotted by JHOC just west of Sunset Cliffs, according to CBP.
SOURCE: 24 August 2017, KGTV San Diego

(U) San Francisco – Canadian Charged in Connection with Yahoo Hack Pleads Not Guilty
(U) A Canadian man charged with aiding Russian hackers accused of breaching a half-billion Yahoo accounts in 2014 has pleaded not guilty before a US judge upon being extradited stateside this week five months after being arrested near Hamilton, Ontario. Karim Baratov entered his plea during a hearing at San Francisco federal court on 23 August, his US-based attorney said. Baratov was arrested under the Extradition Act in March and was subsequently indicted by the US Justice Department on 11 charges connected to an international hacking campaign allegedly orchestrated by Russian intelligence agents. The Russians supplied Baratov with the stolen Yahoo credentials and then hired him to use that information to breach additional internet accounts belonging to various journalists, politicians and private sector employees, according to US prosecutors.
SOURCE: 24 August 2017, The Washington Times

(U) NATIONAL

(U) District of Columbia – TSA Reviewing Cargo Screening, Concerned About Vulnerabilities
(U) Washington – The Transportation Security Administration is reviewing its screening procedures for cargo flown into and within the United States because of concerns that potential security vulnerabilities could be exploited by terrorists. The review, which is examining screening for cargo carried by freight airlines and passenger planes, stems in part from a terror plot that was foiled in Australia last month, according to an official. Investigations revealed that a senior ISIS commander shipped partially

assembled components of a bomb on a commercial cargo plane from Turkey to Australia, according to Australian law enforcement.
SOURCE: 25 August 2017, CNN

(U) Missouri – Man Arrested After Running Over Protestors
(U) St. Louis – A man was charged yesterday after authorities said he pulled his car into a group of demonstrators protesting a police shooting in St. Louis, injuring three people. Mark Colao faces a felony count of resisting arrest by fleeing and misdemeanor charges of leaving the scene of an accident and operating a vehicle in a careless and imprudent manner. Police said the three people suffered minor injuries Wednesday night during a candlelight vigil and protest in honor of Kenny "Kiwi" Herring, who was fatally shot by officers Tuesday after allegedly stabbing one of them.
SOURCE: 24 August 2017, Associated Press

(U) INTERNATIONAL

(U) Bahrain – Bahrain Police Target Terror Cell
(U) Dubai –Bahraini authorities say they have arrested seven people allegedly linked to a Shiite militant group. The Ministry of Interior said yesterday that those arrested were part of a 10-member cell suspected of carrying out terrorist activities. It says the cell is led by Hussain Ali Ahmed Dawood, who is believed to be in Iran and who is a leader in the Ashtar Brigade, which has claimed past bombings and attacks in Bahrain. Bahrain has been roiled by years of low-level unrest following a 2011 uprising led by its majority Shiites against the country's Sunni monarchy.
SOURCE: 24 August 2017, Associated Press

(U) Germany – Germany Ban Far-Left Website Accused of Promoting Violence
(U) Berlin – Germany's Interior Ministry has banned an internet site on allegations it was being used to foment left-wing extremist violence, including at this summer's G-20 summit. Interior Minister Thomas de Maiziere said today the site "linksunten.indymedia.org" was responsible for mobilizing "violent actions and attacks on infrastructure" targets. Among other things, he says the site provided information on how to build gasoline bombs and other incendiary devices with timers. The ban comes less than two months since the G-20 summit in Hamburg, which saw three nights of violence.
SOURCE: 25 August 2017, Associated Press

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLEASE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-874-1100.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.